有限幾何における結合行列のP-Rankとその応用 (群論と組み合せ論)

浜田, 昇

数理解析研究所講究録
178巻 1973年 24-37

有限幾何における結合行列の p-rank とその応用

愛媛大 理　浜田 昇

§1. 序

実験計画法でよく知られている釣合型不完備ブロック計画(BIB design)や部分的釣合型不完備ブロック計画(PBIB design)の結合行列をパリティー・チェックマトリックスとして用いることによって得られる線形符号(以下，それぞれBIBD符号，PBIBD符号という)は majority decoding [10] によって比較的簡単に誤りを訂正出来るという長所がある。符号理論の立場からは同じ程度の訂正能力をもつ符号の中では比較的大きい情報点をもつ符号が望ましい。パラメーター $v, b, r, k, \lambda_1, \lambda_2, \cdots, \lambda_m$, n_i, p^i_{jk} $(i,j,k=0,1,\cdots,m)$ をもつ m associate class の PBIB design の結合行列 N をパリティー・チェックマトリックスとする q 値 PBIBD 符号は majority decoding によって，$s=[r/2\max\{\lambda_1,\lambda_2,\cdots,\lambda_m\}]$ 個の誤りまで訂正可能で，情報点の数 k^* は $v-\mathrm{Rank}_q(N)$ であるから，N のガロア体 $GF(q)$ 上での階数 $\mathrm{Rank}_q(N)$ (以下，q-rank と

いう)が比較的小さい結合行列 N や q の値を求める必要がある。ここに q は素数または，素数のべき乗 $(q=p^n)$ である。

本稿では，BIB design や group divisible (GD) type の PBIB design の中で比較的小さい q-rank をもつ結合行列 N (q の値)とその q-rank を求める。

§2. BIB design の結合行列の P-rank

サイズ(ブロック内の実験単位の個数)が一様に k である b 個のブロックがあって，これに v 個の処理が次の三条件をみたすように割り付けられているとき，これを釣合い型不完備ブロック計画 (Balanced Incomplete Block Design … 略して，BIB design) という.

(i) 各ブロックは k 個の相異なる処理を含む.

(ii) 各処理は r 個のブロックで生起する.

(iii) 任意の二つの処理は，丁度 λ 個のブロックに対として生起する。

五つのパラメーター (v, b, r, k, λ) の間には次の関係がある.

$$vr = bk, \qquad \lambda(v-1) = r(k-1), \qquad v \leqq b, \qquad (2.1)$$

これら v 個の処理と b 個のブロックに適当に番号をつけ，BIB design の結合行列を次のように定義する.

$$N = \| n_{ij} \| \ ; \ i=1,2,\cdots,v, \quad j=1,2,\cdots, b \qquad (2.2)$$

ここに，$n_{ij} = \begin{cases} 1 \ ; & i\text{番目の処理が}j\text{番目のブロックに含まれているとき，} \\ 0 \ ; & \text{そうでないとき．} \end{cases}$

行列 N は (0, 1) 行列であるから，任意の正の整数 n と素数 p に対して，$\mathrm{Rank}_{p^n}(N) = \mathrm{Rank}_p(N)$ が成り立つ．従って，以下 N の p-rank のみを考える．

比較的小さい p-rank をもつ BIB design の結合行列 N や p の値を求めるのに次の定理が役に立つ．

（定理 2.1） N をパラメーター（v, b, r, k, λ）をもつ BIB design の結合行列とする。

(i) p が $(r-\lambda)$ の約数でない素数の場合

(イ) p が r の約数でもないならば，$\mathrm{Rank}_p(N) = v$.

(ロ) p が r の約数ならば，$\mathrm{Rank}_p(N) = v-1$ か v.

特に p が k の約数でもあるならば $\mathrm{Rank}_p(N) = v-1$.

(ii) p が $(r-\lambda)$ の約数である素数の場合

N の p-rank は，N の作り方に関係する．

（証） p を任意の素数，$\mathcal{R}_p(N)$ を N の列ベクトルによって生成される GF(p) 上のベクトル空間とすると，次のようなベクトル $\underline{a}$ と $\underline{b}_i$ $(i=1,2,\cdots,v)$ が $\mathcal{R}_p(N)$ の中に存在する．

$$\underline{a}' = (r, r, \cdots, r), \qquad \underline{b}_i = (\lambda, \cdots, \lambda, \overset{i}{r}, \lambda, \cdots, \lambda)$$

$$r\underline{b}_i' - \lambda \underline{a}' = (0, 0, \cdots, 0, r(r-\lambda), 0, \cdots, 0) \qquad (2.3)$$

$$\underline{b}_1' - \underline{b}_i' = (r-\lambda, 0, \cdots, 0, -(r-\lambda), 0, \cdots, 0) \qquad (2.4)$$

(2.3), (2.4) および $\sum_{i=1}^{v} n_{ij} = k \ (j=1, 2, \cdots, b)$ より (イ), (ロ) が成り立つことがわかる. (ii) が成り立つことを示すために例をあげる.

例1) パラメーター (8, 14, 7, 4, 3) をもつ BIB design には, 全部で, 4つの同値でないデザイン D_i ($i = 1, 2, 3, 4$) が存在する[17].

D_1 : {1248, 2358, 3468, 4578, 5618, 6728, 7138, 3567, 4671, 5712, 6123, 7234, 1345, 2456}

D_2 : {1234, 1256, 1278, 5678, 3478, 3456, 1357, 2457, 2458, 1358, 1467, 1468, 2367, 2368}

D_3 : {1234, 5678, 1256, 1456, 1278, 1478, 1357, 3457, 1368, 3468, 2358, 2458, 2367, 2467}

D_4 : {1248, 2358, 3468, 4578, 5618, 6728, 7138, 2357, 6731, 5174, 3412, 7246, 1625, 4563}

ここに, D_1 の 1248, 2358, … は, D_1 の第1番目のブロックは処理 1, 2, 4, 8 を, 第2番目のブロックは処理 2, 3, 5, 8 を含むことを意味し, デザイン D_1 と D_2 が同値でないとは, 対応する結合行列 N_1 と N_2 に対して, $N_1 = PN_2Q$ となる置換行列の組 (P, Q) が一つも存在しないことを意味する. これらのデザインの結合行列 N_1, N_2, N_3, N_4 の GF(2) 上での rank は, それぞれ, <u>4, 5, 6, 7</u>

であることがわかる．このことは $r-\lambda$ の約数である素数 p に対しては，N の p-rank は N の作り方に関係することを示している。（証明終り）

アフィン幾何 $EG(3,2)$ における点と2-フラットから作られるデザイン $EG(3,2):2$ はパラメーター（8, 14, 7, 4, 3）をもつ BIB design で，その 2-rank は 4 であるから，デザイン $EG(3,2):2$ は D_1 と同値である．従って次の定理をうる。

定理 2.2）（i）パラメーター（8, 14, 7, 4, 3）をもつ2つの BIB design D_1 と D_2 が同値であるための必要かつ十分条件は，すべての素数 p に対して $Rank_p(N_1) = Rank_p(N_2)$ が成り立つことである．ここに，N_1, N_2 はそれぞれデザイン D_1，D_2 の結合行列である．（ii）パラメーター（8, 14, 7, 4, 3）をもつ BIB design の中ではアフィン幾何 $EG(3,2)$ を用いて作られるデザイン $EG(3,2):2$ が最小の p-rank をもつ。

任意のパラメーター（v, b, r, k, λ）に対して，上と同様な結果が成り立つかどうかを調べるために，次の条件（i）または（ii）

$$\left.\begin{array}{l}\text{(i)}\quad 1 \leqq \lambda \leqq 3, \quad 3 \leqq k \leqq 5, \quad r \leqq b \leqq 30 \\ \text{(ii)}\quad v = b, \quad 1 \leqq \lambda \leqq 3, \quad 7 \leqq v \leqq 20\end{array}\right\} \quad (2.5)$$

をみたすパラメーター（v, b, r, k, λ）をもつ BIB design の同値でないものの個数とその p-rank を調べた．（詳しくは浜田[7]を参照）

(表 2.1)

No.	v	b	r	k	λ	$[r/2\lambda]$	$(r-\lambda)$ の約数	同値でないものの個数	その P-rank	幾何学的作り方	個数を求めた人
(1)	6	10	5	3	2	1	3	1	5		Nandi [11]
(2)	7	7	3	3	1	1	2	1	4	PG(2,2):1	
(3)	7	7	4	4	2	1	2	1	3		
(4)	8	14	7	4	3	1	2	4	4, 5, 6, 7	EG(3,2):2	Stanton & Mullin [17]
(5)	9	12	4	3	1	2	3	1	6	EG(2,3):1	
(6)	9	18	8	4	3	1	5	?	?		
(7)	10	15	6	4	2	1	2	3	5, 6, 7		Nandi [11]
(8)	10	30	9	3	2	2	7	?	?		
(9)	11	11	5	5	2	1	3	1	6		Nandi [11]
(10)	11	11	6	6	3	1	3	1	5		
(11)	13	13	4	4	1	2	3	1	7	PG(2,3):1	
(12)	13	26	6	3	1	3	5	2	13, 13		Pasquale [13]
(13)	15	15	7	7	3	1	2	5	5, 6, 8, 8, 8	PG(3,2):2	Nandi [12]
(14)	15	21	7	5	2			不存在			Hussain [9]
(15)	16	16	6	6	2	1	2	3	6, 7, 8		Nandi [11] Hussain [8]
(16)	16	20	5	4	1	2	2	1	9	EG(2,4):1	
(17)	21	21	5	5	1	2	2	2	10, 12	PG(2,4):1	
(18)	25	30	6	5	1	3	5	1	15	EG(2,5):1	

ここに、PG(t, q):μ (EG(t, q):μ) は有限射影幾何 PG(t, q) (アフィン幾何 EG(t, q)) における点を処理と、μ-フラットをブロックとみなすことによって作られる BIB design を表わし、○のついた数字はその行の右に書いた PG(t, q):μ や EG(t, q):μ の p-rank を表わす。(表2.1) から、"PG(t, q):μ や EG(t, q):μ は同じパラメーターをもつ BIB design の中では最小の p-rank をもつであろう" と予想することが出来る。この予想は $q=2$, $\mu=t-1$ の場合には正しいことが示される。一般の場合についてはもっか研究中である。PG(t, q):μ や EG(t, q):μ の p-rank については次の定理が成り立つ。

(定理 2.3) t次元射影幾何 PG(t, q) における点と μ-フラットからなる結合行列 N(q; t, μ) はパラメーター:

$v=(q^{t+1}-1)/(q-1)$, $b=\phi(t,\mu,q)$, $r=\phi(t-1,\mu-1,q)$,

$k=(q^{\mu+1}-1)/(q-1)$, $\lambda=\phi(t-2,\mu-2,q)$, $r-\lambda=q^{\mu}\phi(t-2,\mu-1,q)$

をもつ BIB design (PG(t, q):μ) の結合行列で[1]、その p-rank は、

$$R_{\mu}(t,p^{m})=\sum_{(s_0,\cdots,s_m)\in S_{t,\mu}(p^{m})}\ \prod_{j=0}^{m-1}\ \sum_{i=0}^{L(s_{j+1},s_j)}(-1)^{i}\binom{t+1}{i}\binom{t+s_{j+1}p-s_j-ip}{t} \tag{2.6}$$

によって与えられる。ここに、$q=p^{m}$ で $S_{t,\mu}(p^{m})$ は

$s_m=s_0$, $\quad 0\leqq s_j\leqq t-\mu$, $\quad 0\leqq s_{j+1}p-s_j\leqq(t+1)(p-1)$

($j=0,1,\cdots,m-1$) なる条件をみたす整数の組 ($s_0, s_1, \cdots, s_m$) からなる集合で，$L(s_{j+1}, s_j)$ は $(s_{j+1}p - s_j)/p$ を越えない最大の整数を表わす．証明は省略．詳しくは，浜田[4, 5, 6, 7] を参照のこと

（系）特に，$\mu = t-1$（超平面）の場合には，$N(p^m; t, t-1)$ の P-rank は

$$R_{t-1}(t, p^m) = \binom{p+t-1}{t}^m + 1 \qquad (2.7)$$

である．([15], [16])

（系）$PG(t, p^m)$ における点と μ-フラットからなる結合行列 $N(p^m; t, \mu)$ の 0 元を 1 に，1 を 0 にかえることによって出来る行列 (complement matrix) $N^*(p^m; t, \mu)$ の P-rank は $R_\mu(t, p^m) - 1$ である．

（定理 2.4）アフィン幾何 $EG(t, q)$ における点と μ-フラットからなる結合行列 $M(q : t, \mu)$ はパラメーター：

$$v = q^t, \quad b = \phi(t, \mu, q) - \phi(t-1, \mu, q), \quad r = \phi(t-1, \mu-1, q),$$

$$k = q^\mu, \quad \lambda = \phi(t-2, \mu-2, q), \quad r - \lambda = q^\mu \phi(t-2, \mu-1, q)$$

をもつ BIB design ($EG(t, q) : \mu$) の結合行列で，その P-rank は

$$r_\mu(t, p^m) = R_\mu(t, p^m) - R_\mu(t-1, p^m) \qquad (2.8)$$

で与えられる．ここに，

$$\phi(t, \mu, q) = \frac{(q^{t+1}-1)(q^t-1)\cdots(q^{t-\mu+1}-1)}{(q^{\mu+1}-1)(q^\mu-1)\cdots(q-1)} \qquad (2.9)$$

である[3]．

§ 3. GD type の PBIB design の結合行列の P-rank

(定義) $v = s_1 s_2$ 個の処理 $\phi(i,j)$ $(i=1,2,\cdots,s_1,\ j=1,2,\cdots,s_2)$ の間に次の関係があるとき，v 個の処理の間には 2 associate class の group divisible (GD) type の association scheme が定義されているという [2].

$$\begin{cases} \alpha_1=\beta_1,\ \alpha_2=\beta_2 \text{ ならば，} \phi(\alpha_1,\alpha_2) \text{ と } \phi(\beta_1,\beta_2) \text{ は 0-th associate である．} \\ \alpha_1=\beta_1,\ \alpha_2\neq\beta_2 \text{ ならば，} \quad \text{〃} \quad \text{〃 は 1-st associate である．} \\ \quad \alpha_1\neq\beta_1 \quad \text{ならば} \quad \text{〃} \quad \text{〃 は 2-nd associate である．} \end{cases}$$

(定理 3.1) N をパラメーター $v=s_1 s_2$, b, r, k, λ_1, λ_2, n_i, P^i_{jk} $(i,j,k=0,1,2)$ をもつ GD type の PBIB design の結合行列とする．

(A) $rk - v\lambda_2 \neq 0$, $r-\lambda_1 \neq 0$ (regular GD design) の場合

(i) 素数 P が $r(r-\lambda_1)(rk-v\lambda_2)$ の約数でないならば，$\mathrm{Rank}_p(N) = v$.

(ii) 素数 P が $(rk-v\lambda_2)$ の約数でないならば，$\mathrm{Rank}_p(N) \geqq s_1(s_2-1)$.

(iii) 素数 P が $(r-\lambda_1)$ の約数でないならば，$\mathrm{Rank}_p(N) \geqq s_1 - 1$

(B) $rk - v\lambda_2 = 0$, $r-\lambda_1 \neq 0$ (semi-regular GD design) の場合

P が $(r-\lambda_1)$ の約数でないならば，$s_1(s_2-1) \leqq \mathrm{Rank}_p(N) \leqq s_1(s_2-1)+1$.

(C) $rk - v\lambda_2 \neq 0$, $r-\lambda_1 = 0$ (singular GD design) の場合

P が $(rk-v\lambda_2)$ の約数でないならば，$s_1 - 1 \leqq \mathrm{Rank}_p(N) \leqq s_1$

である

$M_1(g;t,u)$ を $E_J(t,g)$ における原点以外の点 1 この点と原点を

通らないμ-フラットからなる結合行列とすると，(i) $g\neq 2$の場合には，これはパラメーター：

$$v=g^t-1,\quad b=\phi(t,\mu,g)-\phi(t-1,\mu,g)-\phi(t-1,\mu-1,g),\quad k=g^\mu,$$

$$r=\phi(t-1,\mu-1,g)-\phi(t-2,\mu-2,g),\quad \lambda_1=0,\quad \lambda_2=\phi(t-2,\mu-2,g)-\phi(t-3,\mu-3,g)$$

$$n_1=g-2,\quad n_2=g^t-g,\quad P_{11}^1=g-3,\quad P_{11}^2=0,\quad \alpha_1=(g^t-g)/(g-1),$$

$$P_1=rk-\lambda_2 v=g^{\mu-1}\{g^{\mu+1}\phi(t-2,\mu-1,g)-(g^t-1)\phi(t-3,\mu-2,g)\}$$

$$P_2=r-\lambda_1=g^\mu\phi(t-2,\mu-1,g)$$

をもつ regular GD (PBIB) design の結合行列で，(ii) $g=2$の場合には，$M_1(2;t,\mu)$はパラメーター：

$$v=2^t-1,\quad b=(2^t-1)\phi(t-2,\mu-1,2),\quad r=2^\mu\phi(t-2,\mu-1,2),\quad k=2^\mu,$$

$$\lambda=2^{\mu-1}\phi(t-3,\mu-2,2),\quad r-\lambda=2^{\mu-1}\{2\phi(t-2,\mu-1,2)-\phi(t-3,\mu-2,2)\}$$

をもつ B I B design の結合行列である．

（定理3.2） EG(t,g)における原点以外のg^t-1個の点と原点を通らないμ-フラットからなる結合行列$M_1(g;t,\mu)$のP-rankは$R_\mu(t,p^n)-R_\mu(t-1,p^n)-1$である．　ここに$g=p^n$である．

αをGF(g^{t+1})の原始元とし，PG(t,g)の任意のμ-フラットを

$$V(0)=\{(a_0\alpha^{e_0}+a_1\alpha^{e_1}+\cdots+a_\mu\alpha^{e_\mu})\}$$

とする。ここに，$a_0, a_1, \cdots, a_\mu$ は $GF(q)$ の元で，$\alpha^{e_0}, \alpha^{e_1}, \cdots, \alpha^{e_\mu}$ は $GF(q)$ 上で一次独立な $GF(q^{t+1})$ の元である．

$$V(r) = \{(a_0\alpha^{e_0+r} + a_1\alpha^{e_1+r} + \cdots + a_\mu\alpha^{e_\mu+r})\}$$

とおくと，任意の正の整数 r に対して，$V(r)$ も μ-フラットである．

$V(\theta) = V(0)$ となる正の整数 θ を $V(0)$ のサイクルといい，最小の θ を最小サイクル (m.c.) という。$v = (q^{t+1}-1)/(q-1)$ は任意の μ-フラットのサイクルである．$PG(t,q)$ における μ-フラット V が，v よりも小さいサイクル θ をもつならば，$\ell+1$ が $t+1$ と $\mu+1$ の共約数で，しかも $\theta = (q^{t+1}-1)/(q^{\ell+1}-1)$ である正の整数 ℓ が存在する[18]．逆に，$\ell+1$ が $t+1$ と $\mu+1$ の共約数であるような任意の整数 ℓ に対して，$\theta_\ell = (q^{t+1}-1)/(q^{\ell+1}-1)$ をサイクルにもつ μ-フラットが $n_\ell = \phi(t_\ell, \mu_\ell, q^{\ell+1})$ 個存在する．ここに，

$$t_\ell + 1 = (t+1)/(\ell+1), \quad \mu_\ell + 1 = (\mu+1)/(\ell+1)$$

である．$PG(t,q)$ における v 個の点とサイクル θ_ℓ をもつ n_ℓ 個の μ-フラットからなる結合行列を $N(\theta_\ell)$ で表わすと，

(i) $\ell > 0$ の場合には，$N(\theta_\ell)$ はパラメーター：

$v = \phi(t, 0, q)$，$b = \phi(t_\ell, \mu_\ell, q^{\ell+1})$　$r = \phi(t_\ell-1, \mu_\ell-1, q^{\ell+1})$，
$k = \phi(\mu, 0, q)$，$\lambda_1 = \phi(t_\ell-1, \mu_\ell-1, q^{\ell+1})$，$\lambda_2 = \phi(t_\ell-2, \mu_\ell-2, q^{\ell+1})$，
$n_1 = (v/\theta_\ell - 1)$　$n_2 = (v/\theta_\ell)(\theta_\ell - 1)$．$P_{11}^1 = v/\theta_\ell - 2$，$P_{11}^2 = 0$，

$$P_1 = rk - \lambda_2 v = q^{(l+1)\mu_l}\,\phi(t_l-2, \mu_l-1, q^{l+1})(q^{l+1}-1)/(q-1),$$

$$P_2 = r - \lambda_1 = 0$$

をもつ singular GD(PBIB) design である．

(ii) $l=0$ の場合には，$N(\theta_0) = N(q; t, \mu)$ である．

（定理3.3） $PG(t, q)$ の点とサイクル θ_l をもつ μ-フラットからなる結合行列 $N(\theta_l)$ の p-rank は $R_{\mu_l}(t_l, p^{(l+1)m})$ である．ここに $q = p^m$ で，$R_\mu(t, p^m)$ は（2.6）式で与えられる．

（詳しくは，浜田［7］参照） 特に，$l=0$ の場合には，

（系） $PG(t, q)$ における点と μ-フラットからなる結合行列 $N(\theta_0)$（$= N(q; t, \mu)$）の p-rank は $R_\mu(t, p^m)$ である．

参考文献

［1］ Bose, R.C. On the construction of balanced incomplete block designs. Ann. Eugenics 9 (1939), 353-399.

［2］ Bose, R.C. and Shimamoto, T. Classification and analysis of partially balanced incomplete block designs with two associate classes. J. Amer. Statist. Assoc. 47 (1952), 151-184.

［3］ Carmichael, R.D. Introduction to the theory of groups of finite order. Ginn and Company. Boston (1937).

[4] Hamada, N. The rank of the incidence matrix of points and d-flats in finite geometries. J. Sci. Hiroshima Univ. Ser. A-I 32 (1968), 381-390.

[5] 浜田昇 有限幾何における点とd-flatsからなるincidence matrixのrankとmajority decodable codeについて.
数理解析研究所講究録82(1970) 情報理論・実験計画法における組合せ数学の諸問題研究会 報告集108-120.

[6] 浜田昇 有限幾何における結合行列のP-rankとその応用.
日本数学会1972年(秋)統計数学分科会 特別講演 82-100.

[7] Hamada, N. On the P-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error correcting codes. To appear in Hiroshima Math. J. 3 (1973).

[8] Hussain, Q.M. On the totality of the solutions for the symmetrical incomplete block designs: λ=2, k=5 or 6. Sankhyā 7 (1945), 204-208.

[9] Hussain, Q.M. Structure of some incomplete block designs. Sankhyā 8 (1947-48), 381-383.

[10] Massey, J.L. Threshold decoding. MIT Press, Cambridge, Mass. (1963).

[11] Nandi, H.K. Enumeration of non-isomorphic solutions of balanced incomplete block designs. Sankhyā 7(1945), 305-312.

[12] Nandi, H.K. A further note on non-isomorphic solutions of incomplete block designs. Sankhyā 7 (1945), 313-316.

[13] Pasquale, V. DE. Sui sistemi ternari di 13 elementi. Rend. R. Ist. Lombardo Sci. e Lett. (2) 32 (1899), 213-221.

[14] Peterson, W.W. Error correcting codes. John Wiley and Sons, New York (1961).

[15] Smith, K.J.C. Majority decodable codes derived from finite geometries. Inst. Statist. mimeo series 561 (1967), Chapel Hill, N.C.

[16] Smith, K.J.C. On the p rank of the incidence matrix of points and hyperplanes in a finite projective geometry. J. Combinatorial Theory 7 (1969), 122-129.

[17] Stanton, R.G. and Mullin, R.C. Uniqueness theorems in balanced incomplete block designs. J Combinatorial Theory 7 (1969), 37-48.

[18] Yamamoto, S., Fukuda, T. and Hamada, N. On finite geometries and cyclically generated incomplete block designs. J. Sci. Hiroshima Univ. Ser. A-I 30 (1966), 137-149.